In Law with

Technology

LBK &P
LAW FIRM

Cyberzagrożenia i zarządzanie ich ryzykiem w działalności organizacji kościelnych - aspekty praktyczne

adw. Grzegorz Leśniewski

27.05.2026 r.

Agenda

CYBERSEC – POJĘCIE	TYPY RYZYK	CASE STUDY
ZARZĄDZANIE RYZYKIEM	PODSUMOWANIE	Q&A

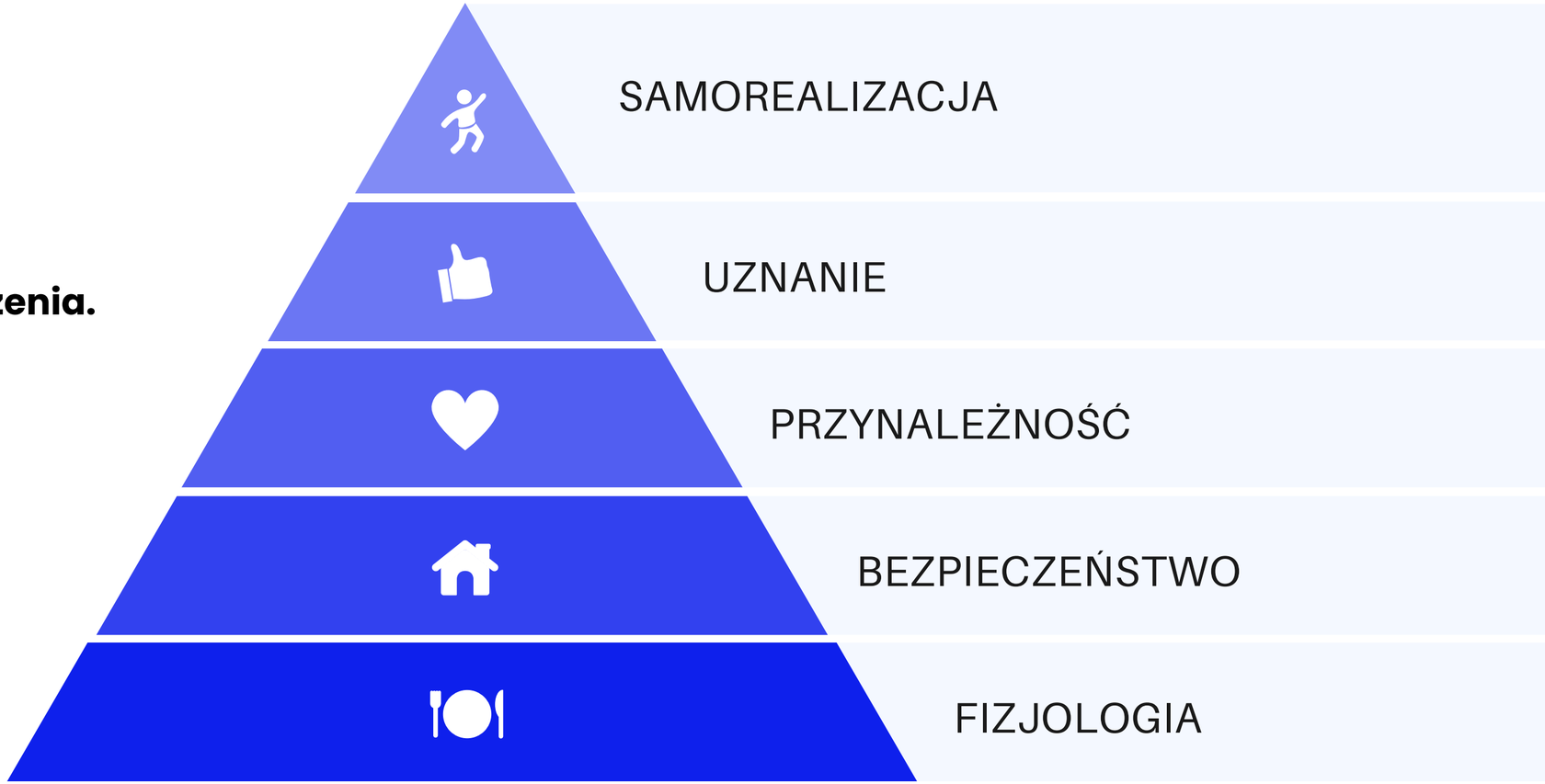
Bezpieczeństwo

LBK &P
LAW FIRM

Ochrona
- **ludzi**
- **zasobów**

przed zagrożeniami.

Stan **pewności**, **spokoju**, **braku zagrożenia.**



Cyberbezpieczeństwo - definicja

LBK &P
LAW FIRM

- “**cyberbezpieczeństwo**”
  działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami

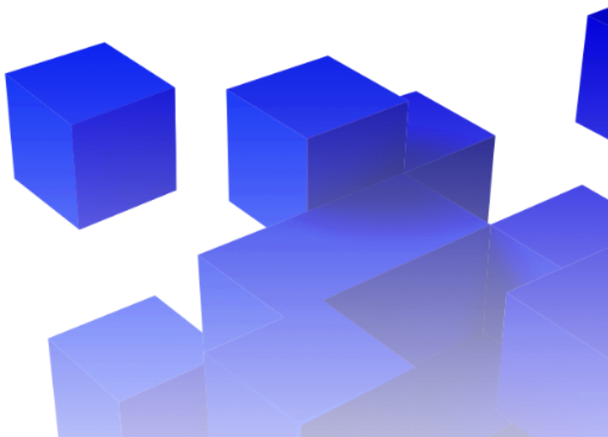
- “**cyberzagrożenie**"
  wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ENISA

Bezpieczeństwo

LBK &P
LAW FIRM

1. zrozumienie ryzyka
2. zabezpieczenia
3. reagowanie/ bcp
4. compliance
5. ubezpieczenie?



Agenda

CYBERSEC – POJĘCIE	TYPY RYZYK	CASE STUDY
ZARZĄDZANIE RYZYKIEM	PODSUMOWANIE	Q&A

Cyber_ryzyka_Polska

LBK &P
LAW FIRM

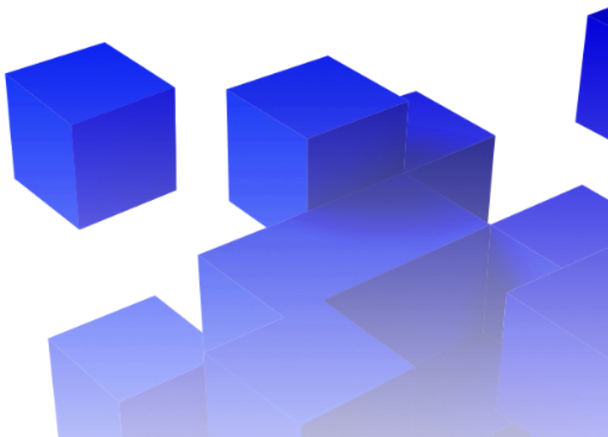
NIE “CZY” - KIEDY

83%

firm zarejestrowało w 2024 roku przynajmniej jeden incydent związany z cyberbezpieczeństwem, co oznacza wzrost o 16 p.p. względem poprzedniego roku.

*Barometr cyberbezpieczeństwa 2025 KPMG

- Wyciek danych za pośrednictwem złośliwego oprogramowania wyprzedził kradzież danych poprzez phishing w rankingu największych cyberzagrożeń.
- Aż 56% przedstawicieli badanych firm uważa, że technologia AI spowoduje wzrost zagrożeń w cyberprzestrzeni.
- Obszary zabezpieczeń, w które firmy planują inwestować w ciągu najbliższych 12 miesięcy:
  1) monitorowanie;
  2)reagowanie na incydenty;
  3)ochrona przed złośliwym oprogramowaniem;
  4) zarządzanie tożsamością i dostępem;
  5) podnoszenie świadomości.



Cyber_ryzyka

ASSET DISCOVERY + ATRYBUTY INFORMACJI

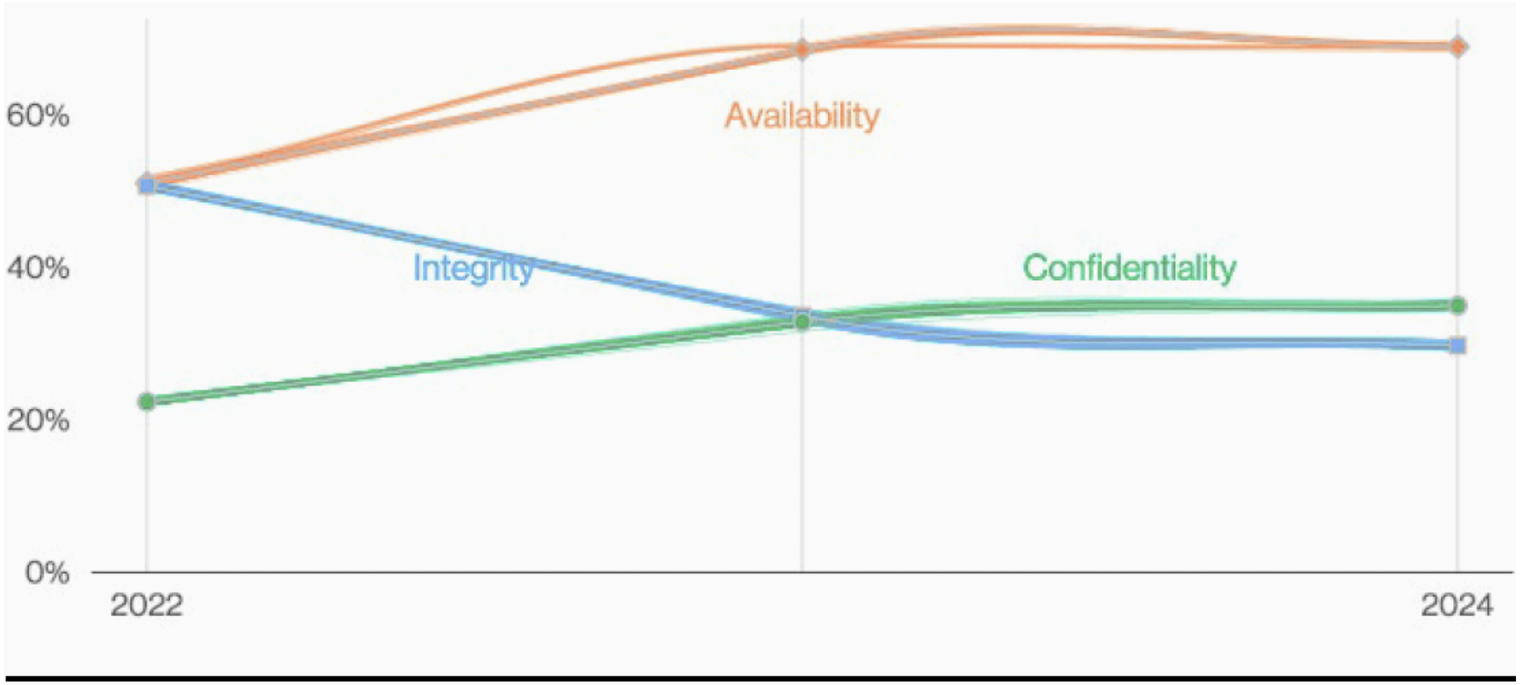


Figure 23. Attributes over time in incidents
verizon business 2024 Data Breach Investigations Report

Cyber_ryzyka

LBK &P
LAW FIRM

Ransomware

Phishing

Malware

SQL Injection

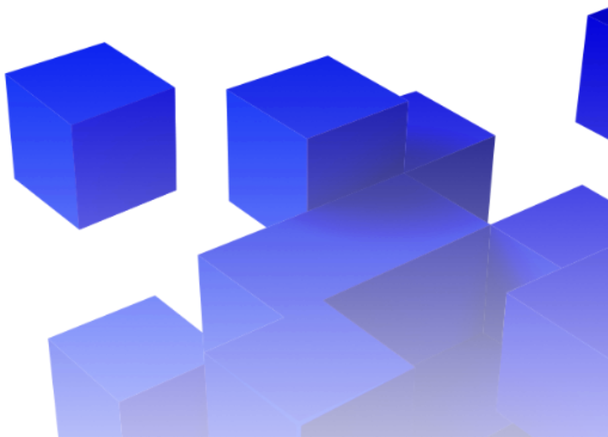
.....

DDoS

Deepfake

Keylogging

Socjotechnika



Cyber_ryzyka

TYPY INCYDENTÓW

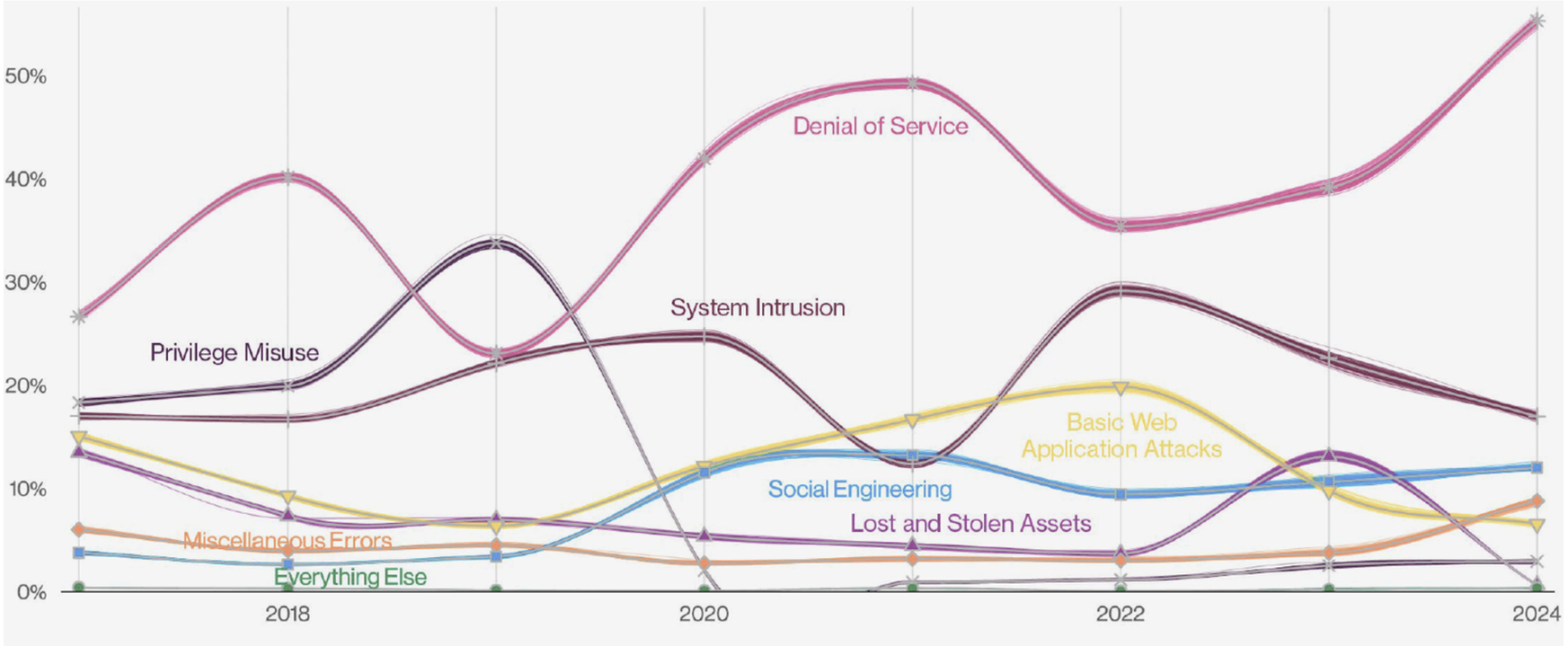


Figure 26. Patterns over time in incidents verizon business 2024 Data Breach Investigations Report

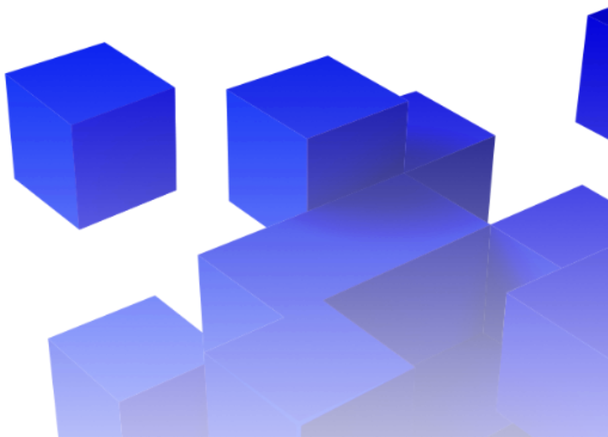
Cyber_AI_future

LBK &P
LAW FIRM

96%

Nearly all respondents are concerned about AI’s impact on the threat landscape.

BItdefender



Cyber_future

LBK &P
LAW FIRM

Table 1. New prioritisation of threats

	THREAT	IMPACT * LIKELIHOOD	IMPACT	LIKELIHOOD
1.	Supply Chain Compromise of Software Dependencies	17,71	4,21	4,21
2.	Skill Shortage	17,20	4,10	4,20
3.	Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems	16,69	3,96	4,22
4.	Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional]	16,21	4,05	4,00
5.	Rise of Digital Surveillance Authoritarianism / Loss of Privacy	15,34	3,96	3,88
6.	Cross-border ICT Service Providers as Single Point of Failure	15,12	4,14	3,65
7.	Advanced Disinformation / Influence Operations (IO) Campaigns	14,38	3,42	4,21
8.	Rise of Advanced Hybrid Threats	14,03	3,68	3,81
9.	Abuse of AI	13,22	3,43	3,86
10.	Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [Optional]	12,99	3,68	3,53
11.	Lack of Analysis and Control of Space-based Infrastructure and Objects	12,52	3,63	3,45
12.	Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data	12,29	3,39	3,63
13.	Increased Digital Currency-enabled Cybercrime [Optional]	10,25	3,06	3,35
14.	Manipulation of Systems Necessary for Emergency Response [Optional]	10,02	3,27	3,07
15.	Tampering with Deepfake Verification Software Supply Chain [Optional]	9,83	3,00	3,28
16.	AI Disrupting/Enhancing Cyber Attacks [Optional]	9,78	3,07	3,19
17.	Malware Insertion to Disrupt Food Production Supply Chain [Optional]	9,33	3,11	3,00
18.	Exploitation of E-health (and Genetic) Data [Optional]	9,32	3,11	3,00
19.	Attacks Using Quantum Computing [Optional]	7,32	2,76	2,65
20.	Disruptions in Public Blockchains [Optional]	5,96	2,47	2,41
21.	Technological Incompatibility of Blockchain Technologies [Optional]	5,91	2,25	2,63

enisa

FORESIGHT CYBERSECURITY THREATS FOR 2030 - UPDATE
March 2024

Agenda

CYBERSEC – POJĘCIE	TYPY RYZYK	CASE STUDY
ZARZĄDZANIE RYZYKIEM	PODSUMOWANIE	Q&A

Ransomware - przykład

LBK &P
LAW FIRM

Atak na Relentless Church i Our Sunday Visitor (USA, 2021)

Szkodliwe pliki przesyłane w ramach phishingu. Atak polegał na zaszyfrowaniu serwerów i baz danych. Relentless Church utracił dostęp do systemów płac i dokumentów, przez co musiał zamknąć swoje szkoły katolickie na kilka dni. Our Sunday Visitor – papierowe prenumeraty i prenumeraty elektroniczne przez kilka tygodni były zakłócone.

Straty: kilkaset tysięcy USD oraz utrata danych

Przeciwdziałanie: edukacja kadry, narzędzia do e-mail filteringu, backupy offline, wieloskładnikowe logowanie i segmentacja sieci

Socjotechnika – przykład

Fałszywe telefony do parafii (Polska, 2022)

Przestępcy dzwonili do księży i przedstawiali się jako policjanci, pracownicy banku lub służb bezpieczeństwa. Twierdzili, że środki znajdujące się na kontach parafialnych są zagrożone (np. przez złodziei lub „zorganizowaną przestępczość”). Namawiali do natychmiastowego przeniesienia pieniędzy na „bezpieczne” konto bankowe.

Straty: kilka milionów złotych, zatrzymano 12 podejrzanych.

Przeciwdziałanie: edukacja, budowanie świadomości, dodatkowe procedury.

Przełamanie hasła – przykład

Włamanie do skrzynki mailowej prezesa Fundacji Solidarności Międzynarodowej (Polska, 2021)

Cyberprzestępcy zhakowali prywatne konto e-mail prezesa fundacji, a stamtąd przejęli również jego profil na Facebooku. Za pomocą kont wysyłano zmanipulowane wiadomości oraz posty propagandowe o rzekomych działaniach polskiego rządu wobec białoruskiej opozycji. Akcja miała wywołać zamieszanie i zaszkodzić wizerunkowi fundacji.

Straty: dezinformacja, wizerunek

Przeciwdziałanie: silne hasła (manager haseł), 2FA

Oszustwo/scam – przykład

LBK &P
LAW FIRM

Oszustwo „kryptowalutowe” – parafia rzymskokatolicka (Żory–Baranowice, 2024–2026)

Ofiara trafiła na ofertę „szybkiego zysku” przez internetową platformę tradingową. Oszuści, podszywając się pod giełdę kryptowalut, nakłonili proboszcza do inwestowania dużych sum (z datków parafian). W rzeczywistości platforma nie istniała; gdy duchowny próbował wypłacić środki, okazywało się, że padł ofiarą oszustwa

Straty: ok. 1 mln PLN

Przeciwdziałanie: edukacja, procedury, weryfikacja podejrzanych ofert

Phishing – przykład

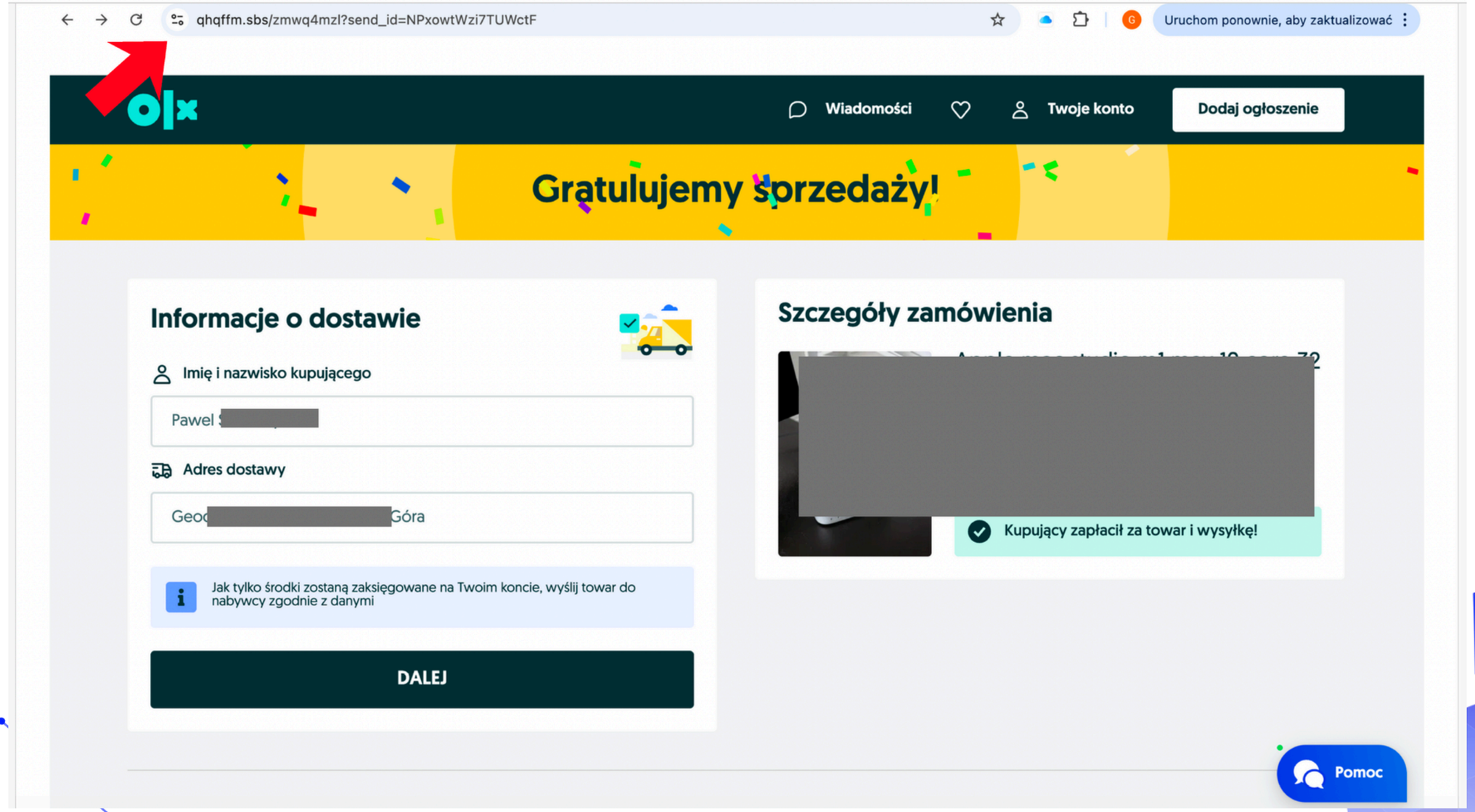
Kampanie phishingowe i inne oszustwa wobec NGO

Organizacje są celem masowych kampanii. Fałszywe e-maile udają komunikaty bankowe („na Wasze konto wpłynie przelew”), sugerujące zainstalowanie załącznika, otwarcie pliku lub zalogowanie się na podrabianej stronie banku. Po kliknięciu ofiary przekazują napastnikom hasła, dane kart płatniczych, wrażliwe informacje.

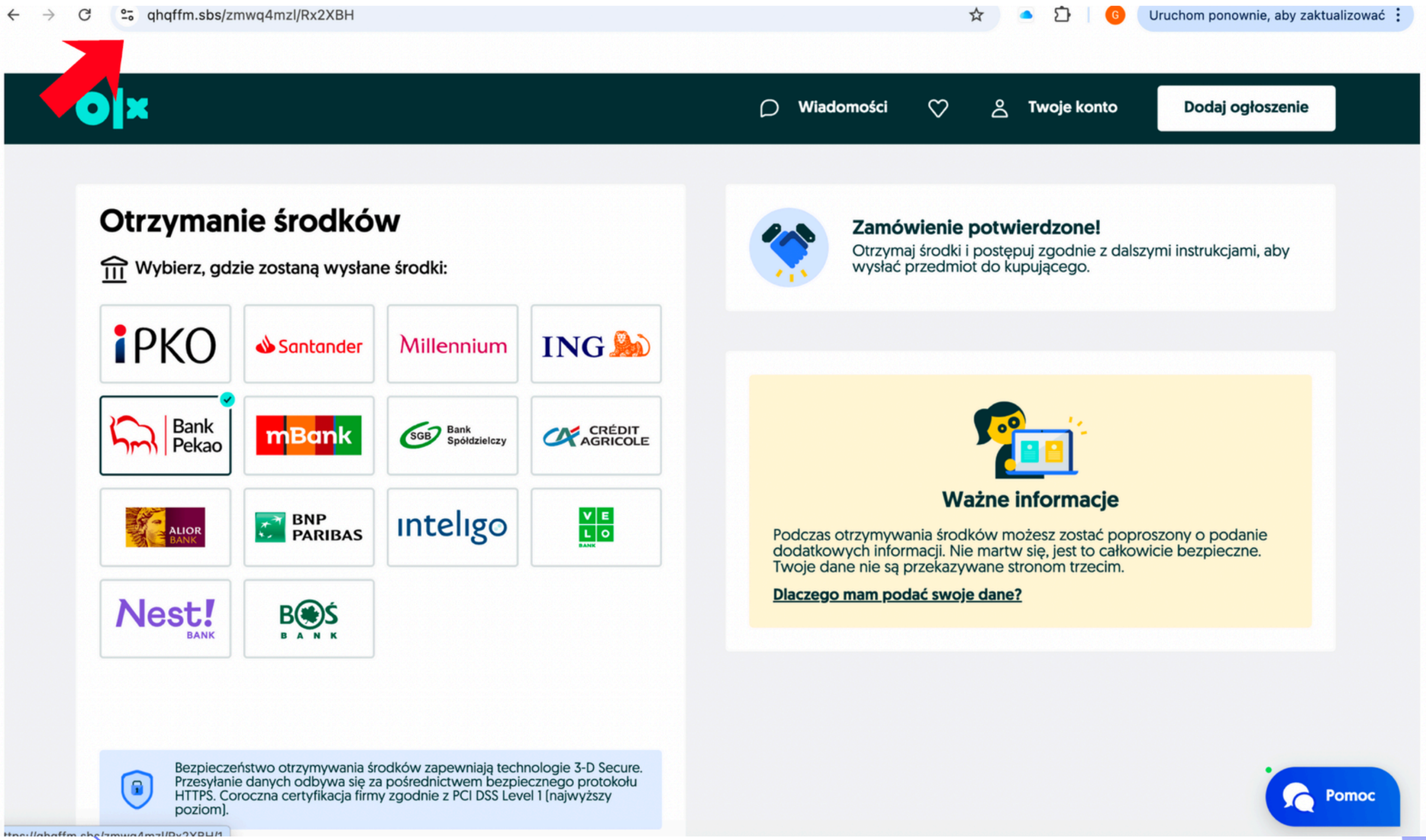
Straty: wielomilionowe

Przeciwdziałanie: edukacja, procedury, 2FA i MFA

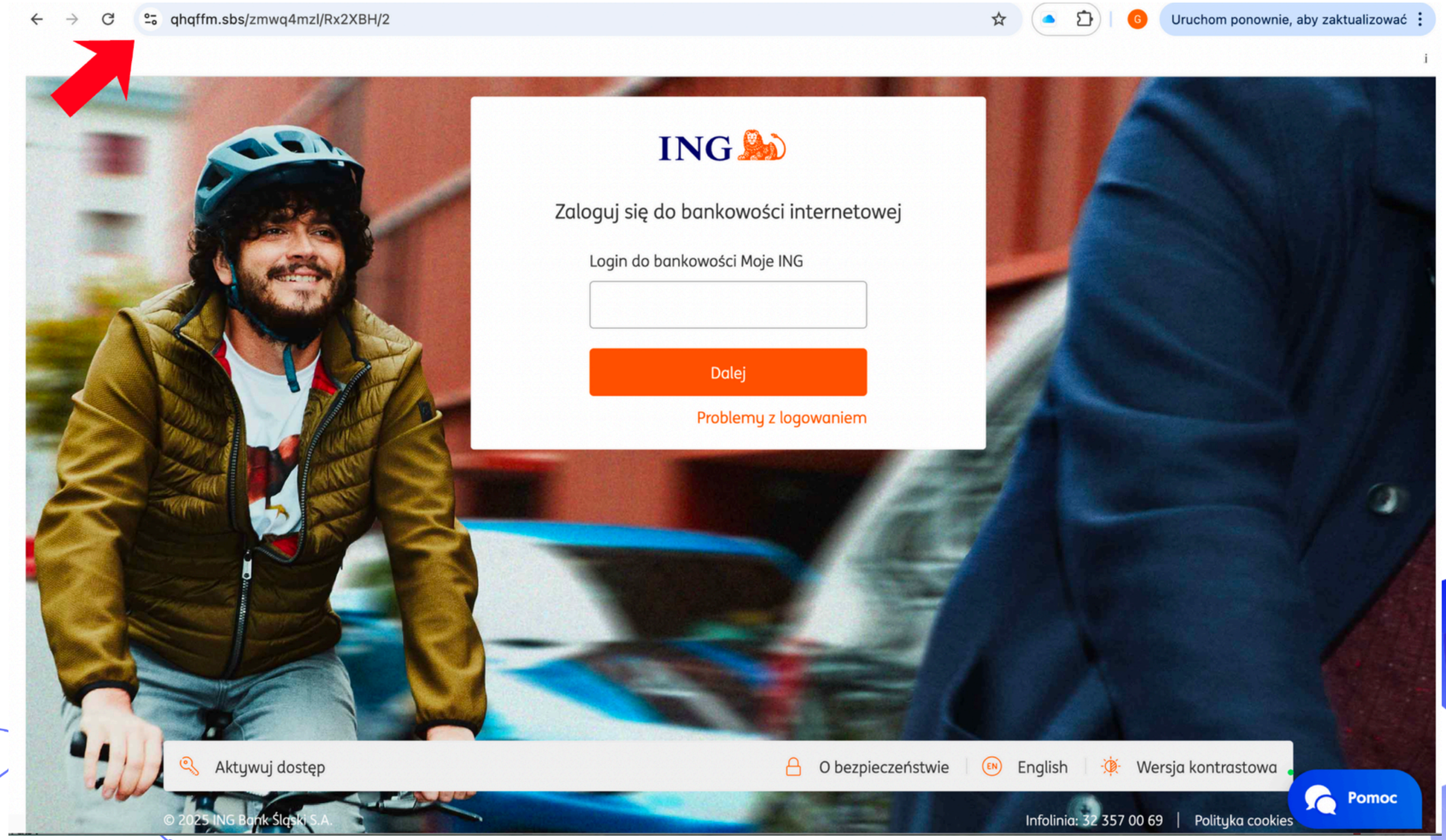
Phishing – przykład



Phishing – przykład



Phishing – przykład



Phishing oraz trojany - przykład

LBK &P
LAW FIRM

Włamanie APT „RedDelta” – Watykan i placówki katolickie w Azji

Kampania cyberwywiadowcza przypisywana chińskiej grupie RedDelta (wpieranej przez państwo). Hakerzy wykorzystali spear-phishing (ukierunkowane ataki mailowe) i zaawansowane narzędzia szpiegowskie (trojany) do przeniknięcia do sieci Watykanu i innych celów katolickich w Chinach.

Straty: pozyskano poufne informacje (np. korespondencję dot. negocjacji Watykan-Chiny)

Przeciwdziałanie: edukacja, narzędzia do e-mail filteringu, wieloskładnikowe logowanie, szyfrowanie i segmentacja sieci, różne poziomy dostępu

Phishing oraz trojany – przykład

LBK &P
LAW FIRM

- **Komitet Międzynarodowy Czerwonego Krzyża (ICRC) – szwajcarskie centrum Działu Poszukiwawczo-Rehabilitacyjnego**
- Hakerzy wykorzystali niezałatany krytyczny błąd w module uwierzytelniania serwerów ICRC (CVE-2021-40539), co pozwoliło im na instalację webshelli i przejęcie uprawnień administratora
- **Straty:** skradziono dane z systemu „Restoring Family Links” – bazy poszukiwanych osób i rodzin. wyciekło ponad 515 tysięcy rekordów osobowych (danych rodzin osób zaginionych lub internowanych), z ponad 90 krajów.
- **Przeciwdziałanie:** testy bezpieczeństwa, bieżące aktualizacje, monitoring sieci (wyciek wykryto po ok. 70 dniach), MFA

Agenda

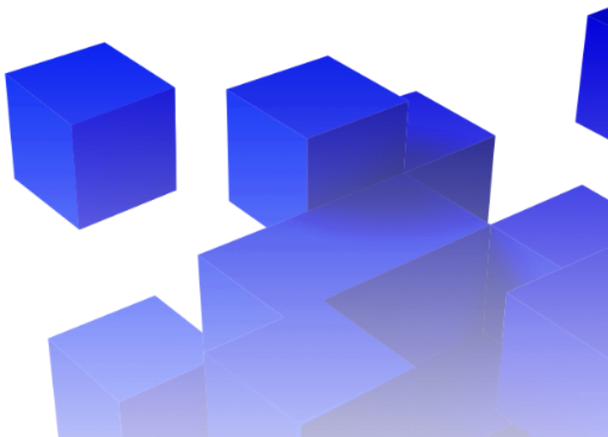
CYBERSEC – POJĘCIE	TYPY RYZYK	CASE STUDY
ZARZĄDZANIE RYZYKIEM	PODSUMOWANIE	Q&A

Ocena ryzyka

LBK &P
LAW FIRM

- **Inwentaryzacja zasobów informacyjnych oraz ich klasyfikacja (ważność)**
  np. bazy danych, urządzenia, aplikacje
- **Identyfikacja zagrożeń**
  np. phishing, ransomware, awarie fizyczne, błędy personelu
- **Identyfikacja podatności (czynniki wzrostu ryzyka)**
  legacy systems, słabe hasła, brak szyfrowania, nieznane procesy, brak szkoleń, rotacja personelu (wolontariusze)
- **Priorytetyzacja**

+ dokumentacja procesu



Szacowanie ryzyka

Ocena prawdopodobieństwa wystąpienia zagrożenia i wpływu na organizację
np. (niski/średni/wysoki lub skala 1–5)

Przykładowa metoda: ryzyko = prawdopodobieństwo × podatność × skutek
np. macierz, tabela do oszacowania ryzyka każdej pary (zasób, zagrożenie)

Zasób	Zagrożenie	Podatność	Prawdopodobieństwo	Wpływ	Ryzyko	Rekomendacja
Serwer z danymi wiernych	Ransomware (szyfrowanie)	Nieaktualne oprogramowanie	Wysokie	Krytyczny	Wysokie	Wdrożyć regularne backupy, aktualizować SW, segmentować sieć
Konto e-mail sekretariatu	Phishing (wyłudzenie hasła)	Brak 2FA, proste hasło	Średnie	Poważny	Średnie	Włączyć 2FA, szkolenie z rozpoznawania phishingu
Obliczenia księgowe (Excel)	Kradzież urządzenia	Brak szyfrowania pliku	Niskie	Poważny	Średnie	Szyfrowanie dysku/plików, polityka silnych haseł
…	…	…	…	…	…	…

Kontrole (ograniczenie) ryzyka

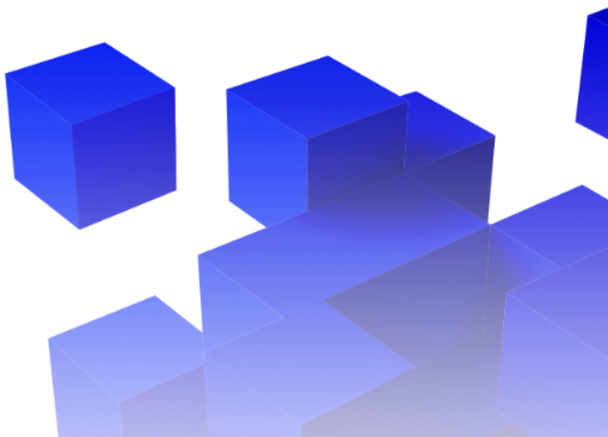
LBK &P
LAW FIRM

- **Zabezpieczenia fizyczne, organizacyjne i techniczne (logiczne)**
- **Absolutne podstawy:** edukacja, budowanie świadomości, antywirus, firewall, szyfrowanie, segmentacja sieci, role based access, kopie zapasowe, 2FA, aktualizacje, managery haseł, polityka dot. urządzeń i narzędzi prywatnych.
- **Procedury ciągłości działania** - plany awaryjne, kopie zapasowe i odzyskiwanie, szkolenia personelu, mocne polityki bezpieczeństwa, zarządzanie dostawcami

Postępowanie z ryzykiem

LBK &P
LAW FIRM

- **Akceptacja** - pozostawienie ryzyka na obecnym poziomie
- **Transfer** - przeniesienie ryzyka na stronę trzecią
- **Redukcja** – wdrożenie dodatkowych środków zmniejszających ryzyko
- **Priorytetyzacja** - najpierw minimalizujemy krytyczne
- **Monitorowanie** – ciągłe śledzenie skuteczności i ocena nowych zagrożeń



Reagowanie na incydenty

LBK &P
LAW FIRM

- **Plan działania** - z góry ustalone procedury
- **Zgłoszenie, klasyfikacja, postępowanie (izolacja, usunięcie, odzyskanie sprawności)**
- **Zgłoszenia formalne** – CERT, PUODO, policja itp. uwaga: często konieczne równolegle do postępowania z incydentem
- **Komunikacja** - informowanie wewnętrzne i zewnętrzne (wizerunek, obowiązki regulacyjne)
- **Analiza** – “lesson learned”

Obowiązki nakładane przez regulacje (przykłady ogólne)

Środki zarządzania ryzykiem w cyberbezpieczeństwie	Zgłaszanie incydentów
Obowiązkowe szkolenia	Powiadamianie pokrzywdzonych o powaznych incydentach oraz środkach zaradczych

rozsądek

Agenda

CYBERSEC – POJĘCIE	TYPY RYZYK	CASE STUDY
ZARZĄDZANIE RYZYKIEM	PODSUMOWANIE	Q&A

LBK &P

LAW FIRM

Grzegorz Leśniewski

Adwokat, Managing Partner

GL@LBKP.PL

+48 531 871 707

Dziękuję za uwagę